



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/821,259	03/29/2001	Mark M. Ishikawa	16057.4002	7236

7590 04/05/2010  
OSAMA HUSSAIN.  
BAY TSP, INC. P.O. BOX 1314  
LOS GATOS, CA 95031

EXAMINER
----------

DURAN, ARTHUR D

ART UNIT	PAPER NUMBER
----------	--------------

3622

MAIL DATE	DELIVERY MODE
-----------	---------------

04/05/2010

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 09/821,259	<b>Applicant(s)</b> ISHIKAWA, MARK M.	
	<b>Examiner</b> Arthur Duran	<b>Art Unit</b> 3622	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 2/1/10.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 54-74 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 54-74 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

## **DETAILED ACTION**

Claims 54-74 have been examined.

### ***Response to Amendment***

The Amendment filed on 5/14/09 is sufficient to overcome the prior rejection.

However, a new 103 rejection has been made.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 54-74 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bezos (6,029,141) in view of Messer (2004/0230491) in view of Ylonen (6782474).

Claims 54, 59, 60, 62, 64, 65, 66, 67, 72, 74:

Examiner notes that Applicant's claims concerning the data interface, data interface provider, and content provider are read in light of Applicant's Specification (Paragraphs [36, 45, 37, 40]).

Bezos discloses combining predetermined Content, an Interface Provider Identification Code, and a Dynamically-Generated User Identification Code to Form a Data Interface, Providing the Data Interface to a User System, and Receiving a Request for Selected Content that is Formed by Combining the Interface Provider Identification

Code and the User Identification Code (Fig. 8; col 15, lines 5-16; col 17, lines 10-29; col 8, lines 16-31; col 13, lines 41-54; col 14, lines 1-11).

Note that Bezos discloses that the advertiser can use any of the predetermined content available from merchant (Amazon) website. And, note that the advertiser presents predetermined content that also includes a link with an advertiser identifier as well as a user identifier.

Bezos further discloses that the url can include data interface provider identification and unique customer identification (Fig. 8). Bezos discloses that the unique customer id can be generated or added to the URL upon the user selecting a referral link (see above citations).

Bezos does not explicitly disclose that the original referral link can include the unique customer ID before selection.

However, Bezos discloses that the unique customer id can be generated or added to the URL upon the user selecting a referral link. And, Bezos discloses that the unique user id can be made a part of the advertising content that is presented to the user as the user shops (Fig. 8 and above citations). And, Bezos discloses that the unique customer ID can be part of the URL for subsequent activity (see above citations) even if the user remains on the original advertiser webpage (col 12, lines 27-41). And, MPEP 2144.04.IV.C discloses that changing the sequence is obvious and MPEP 2144.04.VI discloses that reversal or rearranging of parts is obvious. And, Bezos discloses that the unique user id can be used for tracking and targeting a user (Fig. 1, item 160).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made that Bezos placing the user id in the URL along with the presented advertising information can occur before or after selecting the advertising link. One would have been motivated to do this in order to allow relevant targeting/tracking information on a user to be utilized by the associate/advertiser as well as the merchant or because changing the sequence or reversal or rearranging of parts is an obvious modification.

While Bezos discloses tracking requests for information, Bezos does not explicitly disclose tracking invalid requests for information.

However, Messer discloses tracking and auditing user requests for information:

"[0004] It is an object of the present invention to provide a data processing system for tracking, managing, and auditing select transactions between a plurality of computer workstations interconnected via a common network.

[0013] In order to accomplish these and other objects, the present invention includes a data processing system designed and configured to operate on one or more servers interconnected for communication. The data processing system includes a Clearinghouse server programmed to track, manage, and audit associated transactions of Users clicking-through an Content Provider web site and purchasing a product or service from a Merchant. The Clearinghouse server is also programmed to track and report on the level of activity associated with the Users and produce, on a periodic basis, accounting statements for the participants directed to the transactions that have transpired during the

defined period”.

Messer further discloses tracking both valid and invalid information requests in order to improve commerce on the web:

“[0002]. . .More specifically, the present invention relates to a referral tracking and control system for promoting goods and services on a wide area, public or private access network, such as the Internet .

[0003] As discussed in more detail in the above-referenced parent cases, the present invention includes the ability to track select USER activity while on the Web including interactions with Web pages and click-through navigation to select Web sites where purchases can be executed. Notwithstanding these advancements and advantages, commerce on the web can still be improved upon. Recognizing some of the current difficulties in implementing affiliate programs has led to the innovations presented herein.

[Abstract] An improved processing system for tracking commerce on the Internet provides for subvariable processing and includes web page scanning to discern fraud or improper content to insure proper promotion of select products within the network environment” (Abstract).

Messer further discloses determining invalid requests for information and tracking invalid requests for information, and utilizing a database and reporting for invalid requests for information:

“[0006] It is still another object of the present invention to provide a vehicle

for the detection of affiliate sponsored fraud; exemplary fraud of concern includes use of a process that employs a Javascript to artificially multiply the number of clicks, impressions and/or sales on a banner or similar promotional piece.

[0026]. . In its preferred embodiments, the server is configured with a UNIX operating system. Database management software utilizing Oracle.RTM. on an Apache.RTM.

Webserver is configured for the specific operating system environment. As discussed below, the Clearinghouse is further equipped to deter fraud and other non-productive activity.

[0036] Turning now to FIG. 2, a high level flow chart depicts the programming logic for detecting click fraud. Logic begins at start block 200 and the system at block 210, pulls and enters the next web page in sequence. With the large number of affiliate web pages makes a sequential review perhaps too involve. Accordingly, the system may use a number of sampling techniques, that provide some policing capability. In this way, counter variable I increments the sampled pages and sends these to the scanning program block 220.

[0037] . . . If this test is also positive, the system generates a report, positively identifying the page as a potential source of click fraud., block 250. Logic then continues at 260.

[0038] In addition to the Javascript detection algorithm, the system further tracks potential click fraud by assessing historical patterns of commerce. For example, if a

click-through includes the same ID, the system measures the interval between successive clicks. A relatively fast click speed, or multiple clicks at a uniform interval reflects the possibility that the click is machine generated and potentially fraudulent. Other patterns may give further details, such as large jumps in traffic from individual sites.

[0039] For large scale burst traffic generated from a single or a grouped IP address, within a short interval, the apache server of the Clearinghouse is programmed to block such traffic from hitting the database of the ad servers, thus defending the Clearinghouse server from certain types of DOS (denial of service) attacks. Based on these types of detected activity, the system will create a report and trigger further and more comprehensive evaluations”.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add Messer’s auditing both valid and invalid requests for information to Bezos’ auditing requests for information. One would have been motivated to do this in order to provide prevent fraud, provide better auditing and tracking of information requests, and to provide better commerce on the web.

Additionally, the following is in regards to id expiration. Bezos discloses a shopping cart identifier that can be used to identify a user/computer system (col 8, lines 25-31; col 13, lines 29-41; col 14, lines 51-61) and that the identifier can expire at a set time period (col 2, lines 47-65; col 13, lines 29-41; col 14, lines 51-61). Therefore, Bezos discloses an identifier that expires.



Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made that Bezos user id can expire. One would have been motivated to do this in order to prevent the use of outdated user identifiers.

Additionally, the following is in regards to encryption.

Bezos does not explicitly disclose utilizing different encryption standards for secure communications.

However, Messer further discloses utilizing encryption ([32, 33]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add Messer's utilization of encryption to the prior art's secure communications. One would have been motivated to do this in order to provide standard and readily available technical capabilities for secure communications.

Additionally, Bezos does not explicitly disclose identifying an incoming data request as being associated with a SPAM electronic mail message.

However, Examiner notes that Messer discloses preventing Internet fraud and click fraud related to advertising (Abstract; [6, 14, 36, 37, 38]).

And, Examiner notes that Applicant's Specification states that data requests being associated with a SPAM electronic mail message and click fraud were old and well known in the art (Applicant's Specification [9, 10, 11, 12]). Hence, the Applicant's Specification states that it was old and well known that click fraud can occur from a URL on a webpage or from a URL in an email or from a URL in a SPAM type email.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made that the combination of the prior art and Messer's

identifying click fraud can be applied to websites, emails, SPAM emails. One would have been motivated to do this in order to better identify click fraud.

Additionally, Bezos does not explicitly disclose presenting a dead page to the computer system, the dead page stating that the hyperlink was fraudulently generated.

Examiner notes that Applicant's "dead page" is minimally discussed and minimally mentioned in the Applicant's Specification. Examiner could only find one mention of the term "dead page". In the Summary of the Invention in Paragraph [16], Applicant states, "Additionally, in some embodiments, the user is presented a `dead page` stating that the link was generated fraudulently." (Applicant's Specification, [16]).

However, Messer discloses extensive tracking, reporting, and alerting associated with invalid/fraudulent hyperlink use.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made that fraudulent/invalid URL requests can be returned with a message alerting the user that the request will not be honored. One would have been motivated to do this in order to better discourage fraudulent/invalid requests.

Additionally, in response to Remarks dated 8/8/08, Bezos discloses identifying the user computer and comparing the user computer identification to other computer identifying information to determine which computer this is and whether it is a known or new computer:

"Cookies. A technology that enables a Web server to retrieve information from a user's computer that reveals prior browsing activities of the user. The informational item stored on the user's computer (typically on the hard drive)

Art Unit: 3622

is commonly referred to as a "cookie." Many standard Web browsers support the use of cookies. (col 5, lines 55-60)

Because the identity of the customer is normally unknown to the merchant Web site 106 at the time of the referral event, the site 106 uses cookies technology to identify the customer, so that the customer can be associated with any existing shopping cart created during previous visits to the site 106.

This process involves retrieving the cookie 140 from the customer computer 108 with the Web server 132, and then executing a computer program 144 that compares the cookie against information stored in a customer data structure 148. If no shopping cart exists for the customer, or if no cookie exists on the customer computer 108, a shopping cart structure is created for the user.

Any of a variety of alternative techniques can be used to identify the customer, including prompting the customer for a user ID, and/or using URL information returned by the customer's Web browser. (col 8, lines 15-31)

Upon customer selection of a referral link, the computer program 144 utilizes the customer cookie information 140 passed through an HTTP call to determine whether the particular customer (or technically, the customer computer 108) already has an open shopping cart (event E2). As part of this process, the computer program 144 executes cookie processing software (FIG. 1), which assigns a unique customer ID to the customer based on the cookie information 140. If the customer's Web browser 112 does not support the use of cookies (or if the cookies feature is disabled) the program 144 uses URL

Art Unit: 3622

information received from the Web browser to generate the customer ID.

The customer ID is in turn used by the software 144 to identify any shopping cart currently associated with the customer. If no shopping cart exists for the customer, a new shopping cart structure (which includes the customer ID) is generated within the shopping cart database 152. The customer ID is also stored in a customer database 148. The algorithm used by the program 144 to generate the customer IDs is such that a cookie retrieved from the same customer computer will consistently produce the same customer ID. Thus, assuming the customer always uses the same computer to access the merchant site 106, and that the browser 112 supports the use of cookies, the customer will be assigned the same customer ID, and will be associated with any existing shopping cart.

In one implementation, once the customer has been referred to the merchant site 106 and the customer ID has been determined, the merchant site dynamically includes this ID within hyperlinks of the detail page and other Web pages that are sent to the customer computer 108. When the customer subsequently selects such a link (such as to add a selected product to the shopping cart), the customer ID is automatically transmitted to the merchant site 106 as part of the HTTP message. This allows the merchant site 106 to identify the customer (and shopping cart) without the need to re-request the cookie from the customer computer. (col 13, line 40-col 14, line 10)

The URL (shown at the top of FIG. 8) comprises the unique customer ID 800

(obtained from the customer's cookie or URL information), the product ID 802 (shown as the ISBN of the Terrain Skiing book), the store ID 804 (shown as the "skinet" Web site), and the associate commission ID 806 (the letter "A"). Once the customer has reviewed the product detail page 136, the customer can select the "Add it to your Shopping Cart" hyperlink 808. When the customer clicks on this hyperlink 808, the merchant Web server 132 returns a dynamically-generated HTML document that displays the contents of the shopping cart". (col 15, lines 5-15).

Also, note in the citations above that the cookie is disclosed to identifying the customer computer, "the computer program 144 utilizes the customer cookie information 140 passed through an HTTP call to determine whether the particular customer (or technically, the customer computer 108)". Also, note in the citations above that the computer ID is associated with the cookie, "The algorithm used by the program 144 to generate the customer IDs is such that a cookie retrieved from the same customer computer will consistently produce the same customer ID. Thus, assuming the customer always uses the same computer to access the merchant site 106, and that the browser 112 supports the use of cookies, the customer will be assigned the same customer ID, and will be associated with any existing shopping cart." And, note that the computer ID is dynamically included. And, note that the ID is used for comparison and verification purposes.

Hence, Bezos discloses authenticating a request for data content from a computer system by comparing the computer identification code with the computer identification data, wherein the computer identification code uniquely identifies the

computer system and the computer identification data includes current information for identifying the computer system.

Also, note that Messer also discloses both cookie and IP address utilization in order to verify the identify of a computer:

"[13]... The Clearinghouse server is further programmed to incorporate the use of select tagging of information to permit tracking of web site visitors and for tracking and recording the specific transactions under scrutiny. The identifier typically includes a select coded data and may take the form of a "cookie" (or similar tracking device) that is inserted onto the User's hard disk memory during access to the link. The Clearinghouse server is further programmed to provide a platform for Merchants and Content Providers to efficiently reach terms on their joint promotional and commercial efforts, and for each, to internally monitor these relationships.

[0025] The banner ad is linked, first in a seamless fashion to the Clearinghouse server, block 130. The link then continues directly to the Merchant block 140 (as shown by inner path in FIG. 1). During-the linking process, the USER has an identifier string appended to the HTTP entry, and possibly a "cookie" placed on their system. These act as a marker to permit tracking of the USER by the Clearinghouse, to determine if and when the USER was involved in a purchase, and if to allocate a purchase commission to the Affiliate. The identifier used with select Affiliates include data fields for use to track select information such as a commission vector, i.e., a magnitude

and direction for commission dollars generated by that USER's commerce activity on the Web.

[37]... However, these clicks would have telltale signs, such as originating from the same IP address,

[0038] In addition to the Javascript detection algorithm, the system further tracks potential click fraud by assessing historical patterns of commerce. For example, if a click-through includes the same ID, the system measures the interval between successive clicks.”

Additionally, on 5/14/09, Applicant added the following features to the independent claims:

“ . . .for identifying the computer system that activated the hyperlink . . .  
. . .the computer identification code uniquely identifying a selectively chosen computer system and being dynamically generated upon initialization of hyperlink on the selectively chosen compute system.”

Examiner notes that, on the top of page 11, Applicant states that the claims can not use cookie technology for identification purposes. However, Applicant's Specification specifically states that cookies can be used for identification purposes in the Applicant's invention ([50]).

Also, in regards to representative independent claim 54, the first block of features states that “the computer identification data includes current information for identifying the computer system”. The last block of features states that the “computer identification code is dynamically generated upon initialization of the hyperlink”. Hence, what is the

functional difference between the stated computer identification data and computer identification code? The data contains current information at time of activation of hyperlink. The code is dynamically generated at link selection time. Please see the 112 rejection above.

Also, it is unclear to what hyperlink the last block of features, which begins "wherein the hyperlink incorporates said encrypted confirmation code. . .", applies to. For example, the last block of features could apply to the immediately preceding hyperlink which is sent with the dead page. Or, the last block of features could apply to the first stated hyperlink in the first block of features. If the last block hyperlink feature applies to the first block hyperlink, then it would clarify the claims if the hyperlink distinguishing features followed the relevant hyperlink rather than following a series of if statements.

Hence, as is currently written, the claims are open to a broad interpretation. And, the claims can be interpreted in terms of Applicant's ([16, 44, 48]) from the PG\_Pub version. Applicant's Specification states, "[48] Overall, preferred embodiments of the method of authenticating requests for advertisements, or responses thereto, operates, in part, via dynamic generation of information upon the presentation of information to users and the dynamic generation of new, but similar, information upon the user's request for the data. To validate a user's response, the two information sets are compared in total, or in part."

Hence, Applicant's "initialization" and claim features will be interpreted as an id code which is generated prior to presenting an ad or at time of ad presenting is



Art Unit: 3622

compared to a current id data which is generated at time of selection of a hyperlink within the ad. Or, an id from a sent/presented ad is compared with an id in a selected ad hyperlink.

The prior art does render obvious, "authenticating a request for data content is performed by comparing the computer identification code and the computer identification data. .. The computer identification code of claims 54, 65, and 74 is dynamically generated upon initialization of the hyperlink on the selectively chosen computer system, whereas the computer identification data includes current information for identifying a computer system that activated the hyperlink.

As noted in the rejection above, Bezos discloses tracking identification of a user computer and also tracking whether a user computer is a new or already recognized computer (8:17-31; 13:54-67; and the rejection of the independent claims above). Bezos further discloses sending user id in data sent to the user and user id in data selected by the user (14:1-10; 15:5-15; 13:40-14:10). Bezos does not explicitly disclose comparing user id in data sent to user id in data selected for fraud determining purposes.

Additionally, Bezos further discloses for identifying the computer system that activated the hyperlink (13:40-14:10). Bezos further discloses the computer identification code uniquely identifying a selectively chosen computer system (14:1-10) and being dynamically generated upon initialization of hyperlink on the selectively chosen computer system (7:60-8-31).

Additionally, on 2/1/10, Applicant added the following features to the independent claims:

“ the computer identification code uniquely identifying a predetermined computer system and being dynamically generated when the hyperlink is loaded onto the predetermined computer system, the computer identification data including current information for identifying the computer system that activated the hyperlink, being generated when the hyperlink subsequently is activated by the computer system, and expiring in accordance with a predetermined criteria; . . .

wherein the hyperlink is generated by a self-aware device,”.

Also, Applicant's arguments on 2/1/10 address these features above.

Examiner notes that the underlined part are the newly added features. And, Examiner notes that Applicant's Specification specifically states that cookies can be used for identification purposes in the Applicant's invention ([50]). Also, the claims can be interpreted in light of Applicant's ([16, 44, 48]) from the PG\_Pub version. Hence, the computer id code identifies the computer system and is generated when the hyperlink is loaded. And, the computer id data identifies the computer system and is generated when the hyperlink is activated. Hence, the code identifies when the hyperlink is loaded and the data identifies when the hyperlink is activated. Then, the id code and id data are compared.

And, the prior art renders these features obvious.

Bezos discloses computer id code identifies the computer system and is generated when the hyperlink is loaded (Fig. 8; 5:15). Bezos discloses computer id

data which identifies the computer system and is generated when the hyperlink is activated (Fig. 5; col 13:40-55). Bezos further discloses comparing the id code or the id data to computer identification information (8:15-31).

Bezoes does not explicitly disclose comparing the id code and id data for fraud determining purposes. However, Ylonen discloses dynamically generating an id code at time of loading and comparing the id code to a dynamically generated id data at time of activation for validation purposes(claims 8, 11). Also, Messer (citations above) discloses comparing computer identifiers for fraud detection purposes.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made that Bezos id code generated at hyperlink loading can be compared to the id code generated at hyperlink selection for fraud prevention purposes. One would have been motivated to do this in order to better prevent fraudulent activity.

Also, Applicant stated that "the hyperlink is generated by a self-aware device". Applicant Specification mentions "self-aware" only twice, both on page 10 of the Spec:

"It is to be understood that the identifying indicia generator 24 can be any type of hardware or software that is configured to generate identifying indicia 30. For instance, in one embodiment, the identifying indicia generator 24 is a self-aware device that includes some type of unique identifier, such as for example, a network interface MAC address, or an embedded system identifier, wherein the self-aware device is capable of generating identifying indicia 30."

Hence, a self-aware device is given a broad interpretation and is interpreted as a device that is itself uniquely identified and can generate identifiers. And, Bezos discloses a device that is itself uniquely identified and can generate identifiers (Fig. 8; col 15: 5-20). Note that Bezos identifies the store (item 804) that generates ids and also that the store generates ids (items 800, 806). Hence, the prior art renders obvious a device that is itself uniquely identified and can generate identifiers.

Hence, the prior art renders obvious the features of the Applicant's claims.

Claim 55: Bezos further discloses receiving the request for data at the merchant system (Fig . 1).

Claim 56: Messer further discloses utilizing standard encryption protocols ([32, 33]). Hence, it would be obvious that other or a variety of available and standard encryption protocols can be used. One would be motivated to do this to better offer secure data and to take advantage of commonly available encryption standards.

Claim 57: Bezos further discloses utilizing cookies and IP addresses (col 4, lines 50-55; col 5, lines 55-60).

Claim 58: Bezos further discloses generating interest (Figure 1; col 1, lines 50-60).

Claim 61, 71: Bezos further discloses providing advertising (col 1, lines 36-44).

Claim 63, 73: Bezos further discloses providing remuneration (Abstract).

Claim 68: Bezos further discloses providing supporting communication systems (Figures 1, 2, 4, 5).

Claim 69: Bezos further discloses utilizing networks (Figures 1, 2, 4, 5)

Claim 70: Ylonen (5:35-45) further discloses utilizing wireless communications. Also, the MPEP discloses that making something portable or separable is an obvious variation (MPEP 2144.04.V). Hence, it is obvious that Bezos can utilize wireless communications with Internet communications.

### ***Response to Arguments***

Applicant's arguments with respect to claims have been considered but are moot in view of the new grounds of rejection. Please note the addition of the Ylonen reference above. Also, please note the following.

On 2/1/10, Applicant added the following features to the independent claims:

“ the computer identification code uniquely identifying a predetermined computer system and being dynamically .generated when the hyperlink is loaded onto the predetermined computer system, the computer identification data including current information for identifying the computer system that activated the hyperlink, .being .generated when the hyperlink subsequently is activated by the computer system, and expiring in accordance with a predetermined criteria;. . .

wherein the hyperlink is .generated by a self-aware device,”.

Also, Applicant's arguments on 2/1/10 address these features above.

Examiner notes that the underlined part are the newly added features. And, Examiner notes that Applicant's Specification specifically states that cookies can be used for identification purposes in the Applicant's invention ([50]). Also, the claims can be interpreted in light of Applicant's ([16, 44, 48]) from the PG\_Pub version. Hence, the computer id code identifies the computer system and is generated when the hyperlink is

loaded. And, the computer id data identifies the computer system and is generated when the hyperlink is activated. Hence, the code identifies when the hyperlink is loaded and the data identifies when the hyperlink is activated. Then, the id code and id data are compared.

And, the prior art renders these features obvious.

Bezos discloses computer id code identifies the computer system and is generated when the hyperlink is loaded (Fig. 8; 5:15). Bezos discloses computer id data which identifies the computer system and is generated when the hyperlink is activated (Fig. 5; col 13:40-55). Bezos further discloses comparing the id code or the id data to computer identification information (8:15-31).

Bezos does not explicitly disclose comparing the id code and id data for fraud determining purposes. However, Ylonen discloses dynamically generating an id code at time of loading and comparing the id code to a dynamically generated id data at time of activation for validation purposes(claims 8, 11). Also, Messer (citations above) discloses comparing computer identifiers for fraud detection purposes.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made that Bezos id code generated at hyperlink loading can be compared to the id code generated at hyperlink selection for fraud prevention purposes. One would have been motivated to do this in order to better prevent fraudulent activity.

Also, Applicant stated that "the hyperlink is generated by a self-aware device". Applicant Specification mentions "self-aware" only twice, both on page 10 of the Spec:

“It is to be understood that the identifying indicia generator 24 can be any type of hardware or software that is configured to generate identifying indicia 30. For instance, in one embodiment, the identifying indicia generator 24 is a self-aware device that includes some type of unique identifier, such as for example, a network interface MAC address, or an embedded system identifier, wherein the self-aware device is capable of generating identifying indicia 30.”

Hence, a self-aware device is given a broad interpretation and is interpreted as a device that is itself uniquely identified and can generate identifiers. And, Bezos discloses a device that is itself uniquely identified and can generate identifiers (Fig. 8; col 15: 5-20). Note that Bezos identifies the store (item 804) that generates ids and also that the store generates ids (items 800, 806). Hence, the prior art renders obvious a device that is itself uniquely identified and can generate identifiers.

Hence, the prior art renders obvious the features of the Applicant's claims.

### ***Conclusion***

The following prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- aa) Novicov ( 6275934) discloses relevant id data comparing features;
- a) Johnson (5,813,009) discloses storing invalid requests for information in a database (Fig. 1b; Fig. 3; Fig. 7; Fig. 6; and below):

“(124) If the request for information is rejected during the card/terminal operation, the access card holder will receive a "Not Authorized" message, and the invalid access attempt will be updated on the access card database. If a sufficient number of invalid access attempts are made using any single card, the card will also be invalidated for access until a revalidation routine is performed on the card by an authorized agency.

Art Unit: 3622

(134) Information requests not within the card bearer's authority will receive a "not authorized" message and the invalid access attempt will be updated (block 39) to card database 38";

b) Callaghan (5,737,523) discloses storing invalid requests for information in a database:

"(25) In some implementations, the NFS server 200 may respond to in authentic NFS clients with more severe security measures. By way of example, the NFS server 200 may record in a file and/or on a system terminal that an unauthenticated NFS request 22 was received from NFS client 12. Depending upon the circumstances, the NFS server 200 may determine that the NFS client 12 is attacking and preclude the NFS client 12 from making further NFS requests. One embodiment of step 436 will be described below in more detail with reference to FIG. 10.

(28) Once the export information table 222 has been searched in step 454, a step 456 determines whether the given file system 30 was found in the export information table 222. The given file system 30 is only present in the export information table 222 when the NFS server 200 is making the given file system 30 accessible for sharing. When the given file system 30 is not found in search step 454, control is passed to a step 458 which returns an error message to the NFS client 12. In some embodiments of the present invention, additional or different security measures may be performed. As described above with reference to FIG. 9, these include logging a message on the system terminal, maintaining a file record of unauthenticated client requests, and/or precluding operation of future NFS requests by the NFS client 12";

c) Pines (2005/0143064) discloses storing invalid requests for information in a database:

"[0119] As illustrated in FIG. 5D, those requested changes which cannot be implemented are stored in Rejected Updated Listings Tables 52D along with a reason for the rejection, for example, that the user is an invalid user, and/or that the requested changes is a duplicate, and the like";

d) Wagener (5,793,028) discloses storing invalid requests for information in a database.



Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arthur Duran whose telephone number is (571)272-6718. The examiner can normally be reached on Mon- Fri, 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eric Stamber can be reached on (571) 272-6724. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 3622

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Arthur Duran  
Primary Examiner  
Art Unit 3622

/Arthur Duran/  
Primary Examiner, Art Unit 3622  
3/11/2010